UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

ANÁLISIS GRUPAL: DE UN CIBERATAQUE REAL Y SU IMPACTO EMPRESARIAL

NotPetya– Maersk (2017)

Integrantes:

Donaldo Demián Gómez Arreguín - 179822

Miguel Ángel Aguilar Carrizales - 182318

Josué Emiliano Rosales Ramírez - 181760

Beltrán Reyna David - 183636

Luis Eduardo Aznar Cuevas - 179880

Roberto Emiliano Morales Hernández - 182377

Materia:

CNO V Seguridad Informática

Profesor:

López, Servando

Grupo:

T46A

INTRODUCCIÓN

En el contexto de la digitalización global, una de las principales amenazas a las que se enfrentan las empresas y los gobiernos son los ciberataques, los cuales pueden afectar infraestructura crítica a escala internacional. Estos incidentes pueden tener motivaciones económicas, políticas, estratégicas o de sabotaje, provocando interrupciones graves en servicios esenciales y pérdidas económicas millonarias.

Uno de los casos que evidenció de forma contundente el peligro de los ciberataques a gran escala fue el ocurrido en Ucrania en junio de 2017, conocido como el ataque NotPetya. Dicho ataque paralizó sistemas de transporte, bancarios y energéticos dentro del país. Aunque inicialmente se presentó como un ataque de tipo ransomware, investigaciones posteriores demostraron que su verdadero objetivo era la destrucción de sistemas y el daño operativo, más que la obtención de beneficios económicos mediante extorsión.

Entre las empresas más afectadas se encuentra A.P. Moller-Maersk, una de las compañías de transporte marítimo y logística más grandes del mundo. El ataque paralizó gran parte de su infraestructura tecnológica global, afectando puertos, terminales y operaciones logísticas en múltiples países, y generando pérdidas estimadas entre 200 y 300 millones de dólares.

El presente reporte analiza el ciberataque NotPetya y su impacto en Maersk desde una perspectiva técnica, económica y estratégica, con el fin de comprender la relación directa entre la ciberseguridad, la continuidad operativa y la sostenibilidad económica de las organizaciones.

CRONOLOGÍA

Antecedentes (Antes del 27 de junio)	▪ Actores vinculados a un grupo avanzado de amenazas persistentes (APT) conocido como Sandworm, asociado a la inteligencia militar rusa (GRU), lograron comprometer el servidor de actualizaciones del software de contabilidad ucraniano M.E.Doc. ▪ El código malicioso fue insertado dentro de una actualización legítima y distribuido automáticamente a miles de organizaciones que utilizaban dicho software.
Mañana del 27 de junio de 2017	▪ Miles de empresas en Ucrania instalaron la actualización comprometida de M.E.Doc de forma normal. Al ejecutarse, el malware NotPetya se activó y comenzó a sobrescribir el Master Boot Record (MBR) y a destruir archivos críticos del sistema, dejando los equipos completamente inoperables. ▪ El ataque coincidió con la víspera del Día de la Constitución de Ucrania, lo que amplificó su impacto.
27 de junio de 2017, dentro de Maersk	▪ Los sistemas de tecnologías de la información de Maersk comenzaron a fallar de manera simultánea. El personal de TI tardó aproximadamente dos horas en desconectar la red global para frenar la propagación. ▪ Durante la tarde, sistemas críticos como correo electrónico, SAP ERP, servicios de reservas, logística, estaciones de trabajo y servidores quedaron inutilizados.

	▪ La empresa recurrió a procesos manuales para mantener operaciones mínimas en puertos y terminales mientras iniciaba la reconstrucción de su infraestructura tecnológica.
28 y 29 de junio	▪ Maersk emitió un comunicado oficial confirmando el ataque. ▪ Se lograron restaurar parcialmente algunos sistemas, permitiendo aceptar reservas existentes de clientes.
03 al 09 de julio	▪ Las operaciones de Maersk Line, Damco y APM Terminals comenzaron a normalizarse progresivamente conforme se reconstruían los sistemas afectados.
Investigaciones posteriores	▪ Se confirmó que NotPetya no era un ransomware funcional, sino un malware destructivo diseñado para inutilizar sistemas de forma irreversible, sin posibilidad real de recuperación mediante pago de rescate.

CONTEXTO

NotPetya surge en un contexto de tensión geopolítica en Europa del Este, el ataque se encontraba dirigido inicialmente a Ucrania, usando un software contable muy extendido llamado ***M.E. Doc***, que la mayoría de las empresas ucranianas y organismos públicos utilizaban para obligaciones fiscales y contables**.**

Esta dependencia de un software único, provoco un punto de fallo sistémico, donde si ese programa se veía comprometido, la red de la empresa u organismo se veía afectada

Por lo que el 27 de junio del 2017, ocurrió la empresa Moller-Maersk dependiente de ese software, una actualización en M.E. Doc fue ejecutada, y por consiguiente la red dentro de la empresa fue comprometida (junto a la de otras)

Vulnerabilidades y Condiciones
Cadena de suministro comprometida ▪ El ataque no fue por *phishing* convencional ni por un fichero malicioso descargado por error, los atacantes infiltraron el proceso de actualización de M.E.doc, insertando *NotPetya* dentro de un software que millones de sistemas confiaban de forma automática, aplicando lo que se conoce como ***Supply Chain Attack****,* siendo un ataque a la cadena de suministro, donde el malware se instala en una actualización legítima y se propaga a través de ella.
Errores y negligencias de M.E.doc ▪ La empresa M.E.doc había sido advertida por firmas de ciberseguridad sobre vulnerabilidades en sus infraestructuras, pero aparentemente no tomó medidas suficientes para reforzarlas. ▪ El servidor de actualizaciones fue comprometido sin mecanismos adecuados de verificación criptográfica de integridad
Fallas técnicas y de gestión ▪ Sistemas sin parches a vulnerabilidades explotables (Eternalblue). ▪ Redes corporativas sin segmentación efectiva. ▪ Gestión de credenciales y privilegios insuficiente. ▪ Backups no aislados ni actualizados de forma segura.

ELEMENTO	DESCRIPCIÓN
Tipo de ataque	Wiper disfrazado de ransomware. Aunque se presentaba como ransomware (NotPetya), su diseño impedía la recuperación de la información, por lo que su objetivo real fue sabotaje y destrucción de sistemas, no extorsión.
Actor o grupo atacante	Atribuido por EE. UU., Reino Unido y otros países a actores estatales rusos (GRU / APT relacionado con Sandworm). No fue un grupo criminal tradicional.
Vector de entrada	Actualización maliciosa del software contable ucraniano MeDoc (ataque a la cadena de suministro). Maersk tenía una oficina en Ucrania que utilizaba MeDoc, lo que permitió el acceso inicial.
Vulnerabilidad explotada	Compromiso previo de los servidores de actualización de MeDoc. Uso de EternalBlue y EternalRomance para propagación lateral.
Etapas del ataque (MITRE ATT&CK)	El ataque NotPetya contra Maersk puede analizarse utilizando el marco MITRE ATT&CK, el cual describe las tácticas y técnicas empleadas por los atacantes a lo largo del ciclo del ataque: • **Acceso inicial (Initial Access):** Compromiso de la cadena de suministro mediante una actualización maliciosa del software contable M.E.Doc, instalada de forma legítima en sistemas de Maersk en Ucrania. • **Ejecución (Execution):** Ejecución automática del código malicioso al instalar la actualización comprometida del software. • **Persistencia (Persistence):** NotPetya no buscaba persistencia prolongada, ya que su objetivo era la destrucción inmediata de los sistemas. • **Escalada de privilegios (Privilege Escalation):** Uso de credenciales robadas y explotación de vulnerabilidades del sistema para obtener privilegios administrativos. • **Movimiento lateral (Lateral Movement):** Propagación rápida dentro de la red corporativa mediante herramientas como EternalBlue y EternalRomance, así como el uso de credenciales internas. • **Impacto (Impact):** Sobrescritura del Master Boot Record (MBR) y cifrado de archivos críticos, provocando la inutilización total de los sistemas afectados.
Sistemas o servicios comprometidos	▪ Servidores corporativos centrales ▪ Sistemas ERP (SAP) ▪ Sistemas de correo electrónico ▪ Sistemas de reservas y logística ▪ Estaciones de trabajo del personal ▪ Infraestructura de TI en puertos y terminales ▪ Servicios internos de autenticación y directorio activo
Duración del incidente	10 a 14 días.
Mecanismos de detección y respuesta	▪ Detección inicial por fallos masivos simultáneos. ▪ Aislamiento físico de redes. ▪ Apagado de sistemas globales. ▪ Recuperación desde backups offline ▪ Respuesta interna y apoyo de expertos externos en ciberseguridad.

EVALUACIÓN DE IMPACTO

Principio	Descripción del impacto	Evidencia del caso
Confidencialidad	Aunque NotPetya no estaba diseñado para exfiltrar información, el control administrativo total de la red implicó un alto riesgo de exposición de datos sensibles.	Acceso completo a sistemas internos, Active Directory y servidores corporativos.
Integridad	La integridad de los sistemas fue severamente comprometida; archivos, configuraciones y estructuras críticas fueron destruidas de manera irreversible.	Sobrescritura del MBR, corrupción de sistemas SAP y pérdida total de sistemas operativos.
Disponibilidad	La disponibilidad fue el principio más afectado; las operaciones globales de la empresa quedaron paralizadas durante varios días.	Interrupción de puertos, reservas, logística y comunicaciones internas a nivel mundial.

COSTO TOTAL

El modelo económico propuesto por Adrian Mizzi resulta especialmente útil para analizar el impacto del ciberataque NotPetya en Maersk desde la perspectiva de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este modelo permite evaluar si la inversión en controles de seguridad fue adecuada al comparar los costos de prevención con los costos derivados de un incidente de seguridad.

En el caso de Maersk, los costos de construcción y protección de la seguridad (segmentación de red, auditoría de proveedores y backups aislados) fueron significativamente menores en comparación con los costos de ruptura, pérdida de ingresos y reconstrucción de la infraestructura tecnológica, los cuales superaron los 300 millones de dólares. Esto evidencia que la organización se encontraba en un punto de inversión subóptimo en materia de seguridad de la información.

El modelo de Mizzi complementa los marcos del SGSI como ISO/IEC 27001, al aportar una visión económica que justifica la necesidad de invertir de manera proporcional al impacto potencial de las amenazas.

Tipo de costo	Descripción	Estimación (MXN)
Pérdidas operativas	Inactividad global de operaciones logísticas, puertos y servicios durante aproximadamente dos semanas.	**$3,500,000,000 MXN**
Daños reputacionales	Deterioro de confianza de clientes, percepción de riesgos, impacto en imagen de marca y posibles efectos en contratos y alianzas logísticas	**$800,000,000 MXN**
Costos técnicos	Recuperación de sistemas y consultorías externas; reinstalación de entre 4000 servidores, 45000 PCs y 2500 aplicaciones	**$1,100,000,000 MXN**
Costos legales / regulatorios	No hubo sanciones conocidas específicas contra Maersk por regulación como GDPR	**$0 MXN**
Pago de rescate o extorsión	NotPetya se presentó como ransomware pero no tuvo mecanismos funcionales de rescate real; no se pagó rescate.	**$0 MXN**
TOTAL ESTIMADO	300 millones USD × tipo de cambio promedio 2017 (~18 MXN).	300 million USD * 18 **$5,400,000,000 MXN** (cinco mil cuatrocientos millones de pesos mexicanos) (Considerando el año de 2017)

MARCOS NORMATIVOS

El incidente de NotPetya evidenció la importancia de aplicar de forma efectiva marcos normativos internacionales de ciberseguridad:

- ***ISO/IEC 27001***

Controles como A.12 (gestión de vulnerabilidades), A.13 (seguridad en redes y segmentación) y A.17 (continuidad del negocio) pudieron haber mitigado la propagación del malware y reducido el impacto global.

- ***NIST Cybersecurity Framework***

Las funciones Identify y Protect fallaron al no evaluar adecuadamente riesgos de terceros; Detect fue limitada debido a la propagación acelerada; Respond y Recover demostraron la importancia de planes de respuesta y respaldos offline.

- ***BCP y DRP***

La ausencia de respaldos completamente aislados incrementó el tiempo de recuperación, evidenciando la necesidad de planes robustos de continuidad y recuperación ante desastres.

LECCIONES APRENDIDAS Y RECOMENDACIONES

El ataque NotPetya dejó lecciones clave para Maersk y para organizaciones con infraestructuras digitales complejas:

- ✓ *La seguridad no depende únicamente de sistemas internos, sino también de la evaluación continua de proveedores y terceros.*
- ✓ *Las arquitecturas de red sin segmentación convierten incidentes locales en fallas globales.*
- ✓ *Los respaldos deben estar aislados y protegidos contra ataques destructivos.*
- ✓ *La gestión oportuna de parches reduce el riesgo de explotación de vulnerabilidades conocidas.*
- ✓ *Los planes de respuesta a incidentes y continuidad del negocio son críticos para minimizar impactos económicos.*

En el contexto mexicano y latinoamericano, donde muchas empresas dependen de software fiscal o gubernamental obligatorio, resulta fundamental auditar a proveedores tecnológicos, fortalecer controles de seguridad y fomentar una cultura organizacional de ciberseguridad.

REFERENCIAS

- CNBC. (2017, 16 de agosto). Maersk says NotPetya cyberattack could cost $300 million. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
- Computer Weekly. (2017, 16 de agosto). NotPetya attack cost up to $300m, says Maersk. https://www.computerweekly.com/news/450424559/NotPetya-attack-cost-up-to-300m-says-Maersk
- Cyber Peace Institute. (2018). The Untold Story of NotPetya: The Most Devastating Cyberattack in History. https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf
- Cybersecurity simplified. (2020, 12 de septiembre). NotPetya: The biggest cyber attack explained [Video]. YouTube. https://youtu.be/7EGfxPa4nmg?si=CqoO2r3_KH09euEc
- DIARIO OFICIAL DE LA FEDERACIÓN (D.O.F.) (2017). Indicadores económicos de tipo de cambio – Tipo de cambio promedio anual 2017. https://dof.gob.mx/indicadores_detalle.php?cod_tipo_indicador=158&dfecha=01/01/2017&hfecha=31/12/2017#gsc.tab=0
- EJIL: Talk! Blog of the European Journal of International Law. (2017). The NotPetya cyber operation as a case study… https://share.google/8ESa6MUf5oueSNCv4
- InfoSec Academy. (2021, 5 de febrero). NotPetya case study – Maersk cyberattack explained [Video]. YouTube. https://www.youtube.com/watch?v=CLYjs37LT74
- LRQA. (s. f.). NotPetya ransomware attack on Maersk – Key learnings. https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/
- SecurityHive. (s. f.). Hack in practice: The NotPetya attack on Maersk. https://www.securityhive.io/blog/hack-in-practice-the-notpetya-attack-on-maersk
- Schmitt, M., & Biller, J. (2017, 11 de julio). The NotPetya cyber operation as a case study of international law. EJIL: Talk! Blog of the European Journal of International Law. https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/
- U.S. Department of the Treasury. (2018, 15 de febrero). Treasury sanctions Russian Federal Security Service enablers. https://home.treasury.gov/news/press-releases/sm0410